



DEPARTMENT OF THE ARMY
U.S. ARMY MANEUVER SUPPORT CENTER AND FORT LEONARD WOOD
320 MANSCEN LOOP STE 316
FORT LEONARD WOOD, MISSOURI 65473-8929

REPLY TO
ATTENTION OF

ATZT-IM

16 FEB 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy #41-06, Network Access, Use Monitoring, and Information Assurance

1. REFERENCES.

- a. AR 25-1, Army Information Management.
- b. AR 25-2, Information Assurance.

2. GENERAL.

a. This policy establishes oversight responsibility for all Information Systems (IS), network access control, and IS use-monitoring, to the Directorate of Information Management (DOIM). Effective operation and capacity planning for IS requires the vigilant analysis of ongoing network and computer usage. Measurements from this analysis are used to identify, isolate, and repair IS related problems before such failures affect mission readiness or propagate through Army networks.

b. Safeguarding our networks and computer resources necessitates having an effective Information Assurance (IA) program. The FORT LEONARD WOOD IA program begins with astute users who understand use limitations and take responsibility for their actions. The DOIM Information Assurance Manager (IAM) manages the FORT LEONARD WOOD IA program and provides oversight to all organizational Information Assurance Security Officers (IASOs).

c. The Fort Leonard Wood network is an enclave of the Army's Global Information Grid (GIG). The operation and maintenance of our technology infrastructure must comply with policies and procedures established by the United States Army Network Enterprise Technology Command (NETCOM). The DOIM is designated as the Chief Information Officer and must ensure NETCOM and Army IS standards are complied with across our infrastructure.

3. POLICY/PROCEDURES.

a. Commanders/Directors will appoint primary and alternate IASOs who will diligently execute their duties and responsibilities as outlined in reference

b. The IASOs are responsible for proper issuance of network user IDs, user training, and the implementation of all IA policies within their command.

c. In accordance with AR 25-2, Installation Management Agency (IMA), and NETCOM policies, no IS shall be procured, configured, or connected to the FORT LEONARD WOOD infrastructure outside of the operational control of the DOIM. When new technologies or capabilities are required customers must coordinate with the DOIM to ensure solutions are compliant with existing infrastructure designs, hardware and software standards, and are supportable within resource constraints.

ATZT-CG

SUBJECT: Command Policy #41-06, Network Access, Use Monitoring, and Information Assurance


d. Systems fielded to Fort Leonard Wood from external agencies must submit appropriate documents to the DOIM prior to receiving network connectivity. Documents include a Networthiness Certificate, Certificate To Operate, and an Accreditation Plan. The Project Manager in charge of fielding such systems should contact the Fort Leonard Wood IAM for deployment coordination well in advance of their anticipated date of use.

e. All users of Fort Leonard Wood IS must sign and agree to the terms of use prescribed in the Fort Leonard Wood Acceptable Use Policy (AUP) prior to receiving authorized access. Any breach of the AUP will result in the immediate suspension of user privileges. Reinstatement of privileges can be requested after the user receives supplemental IA training from their IASO. Written requests for reinstatement must be submitted to the IAM under the signature of the individual's Battalion level Commander or Organization Director. The request must affirm that remedial training has been conducted, and indicate the disposition of disciplinary action taken in the incident. Violators of the AUP and/or related IS regulations should anticipate a minimum suspension of two weeks.

f. Incidental to the data collection identified in 2 a., the DOIM may discover unauthorized activities as outlined in the AUP and referenced regulations. If such activities are discovered the user account associated with the violation will be suspended. The incident will then be turned over to the unit IASO, commander/director, or proper investigative authorities for action as may be warranted by the nature of the unauthorized activity.

4. SUPERSESSION. This policy is in effect until superseded or rescinded and supersedes policy letter 41-01, Network Access, Internet Use and Internet Monitoring, dated 31 October 2001.

5. PROPONENT. The proponent for this command policy is the DOIM, 563-6113.


RANDAL R. CASTRO
Major General, USA
Commanding

DISTRIBUTION:

All Brigades, Battalions, Companies,
Detachments, Tenant Units, Directorates,
Personal Staff Offices, And Contractors

Acceptable Use Policy

- 1. Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the Fort Leonard Wood Campus Area Network (CAN), a sub-network of the Army Non-secure Internet Protocol Network (NIPRNET), from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.
- 2. Access.** Access to this network is for official use and authorized purposes as set forth in DOD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.
- 3. Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.
- 4. Unclassified information processing.** The Fort Leonard Wood CAN and the NIPRNET are the primary unclassified Information System (IS) for Fort Leonard Wood. The NIPRNET is a system approved to process For Official Use Only (FOUO) collateral information only.
 - a. The Fort Leonard Wood CAN provides unclassified communications to external DOD and other United States Government organizations. Primarily this is done via electronic mail and Internet networking protocols such as *web*, *ftp*, and *terminal emulations*.
 - b. The Fort Leonard Wood CAN and the Internet, as viewed by the Directorate of Information Management (DOIM), are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.
- 5. Minimum security rules and requirement.** All Fort Leonard Wood CAN and NIPRNET users must understand and comply with the security rules and requirements described below prior to gaining access to IS resources:
 - a. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.
 - b. I will generate, store and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lower case letters, numbers, and special characters. I am the only authorized user of this account. I will not use commonly known words, acronyms, names, birthdays, or phone numbers as part of my password or pass-phrase.
 - c. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.
 - d. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, or electronic storage device.
 - e. I will not attempt to access or process data exceeding the authorized IS classification level.
 - f. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.
 - g. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, .bat files) without authorization, nor will I write malicious code.

h. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated, and will not disseminate it to anyone without a specific need to know.

i. I will not utilize Army or DOD provided IS for commercial financial gain or illegal activities.

j. Authorized personnel will perform all network, computer, and peripheral maintenance only.

k. I will use screen locks and log off the workstation when departing the area.

l. I will immediately report any suspicious output, files, shortcuts, or system problems to my unit Information Assurance Security Officer (IASO) and the DOIM Help desk (3-4357 or help@wood.army.mil), and cease all activities on the system.

m. I will address my questions regarding policy, responsibilities and duties to my unit IASO and Chain of Command. Issues that cannot be resolved through my local support personnel will be directed to the installation Information Assurance Manager (IAM) located in the DOIM.

n. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

o. I understand that monitoring of the Fort Leonard Wood CAN is conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities, while not all inclusive, define examples of unacceptable use of Army IS:

(1) Chat Room programs; e.g. services at ICQ, AOL, Excite, Yahoo, etc.

(2) Pager and Instant/Immediate Messaging programs

(3) On-line buying/selling outside of official duties; i.e. E-bay, web stores, stock trading.

(4) Checking personnel E-mail accounts; e.g. services offered by your local Internet service provider, Hotmail, Yahoo, AOL, etc.

(5) On-line gaming and entertainment services.

(6) Sending or proliferating unwanted, unofficial email, also known as SPAM and chain letters.

(7) Transmitting messages with derogatory or inflammatory remarks about a person's race, color, sex, age, disability, religion, national origin, physical attributes, or sexual preference.

(8) Using E-mail to solicit personal transactions; i.e. selling, buying, or giving away personal assets (vehicles, tickets, jewelry, etc.)

(9) Downloading, installing, or using peer to peer (P2P) software on a Government computer or network. (i.e. Kazaa, winmx, morpheus, audio galaxy, imesh, limewire, bearshare)

p. The authority for soliciting your social security number (SSN) is EO9397. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to the Fort Leonard Wood CAN and its information systems.

6. Acknowledgement. I have read the above requirements regarding use of the Fort Leonard Wood IS. I understand my responsibilities regarding these systems and the information contained in them.

Employee Name,

Signature

Date

Unit ISSO Name,

Signature:

Date